INFORMATION TECHNOLOGY SERVICES 6-0000

SERVICES PROVIDED 6-0010

The Information Technology Services Division provides or coordinates the acquisition of the full range of Information Technology services. This includes the development, production, and maintenance of automated Information Technology systems. It is also responsible for departmental compliance with Department of Finance requirements related to Information Technology, as defined by the State Administrative Manual.

Specific reporting requirements from Department of Finance and/or Department of General Services must be completed prior to procurement of IT services, software, or hardware. Extensive delays will occur if reporting requirements are not addressed early. Please contact the Information Technology Services Division if you plan to procure contract support. IT provisions may apply even if the item of computer Information Technology is considered to be a minor portion, or incidental, to the overall contract.

ALLOCATION OF SERVICES 6-0020

The Information Technology Services Division operates on a cost reimbursement basis. The total Information Technology resources available are annually allocated to departmental programs. This allocation process, which involves the deputy directors, Budget Office, and executive staff, is based on needs as defined by programs.

Additional Information Technology resources may be secured through the Budget Change Proposal (BCP) process. The Information Technology Services Division has the responsibility to assist and coordinate these processes with departmental programs. The Department of Finance requires that our Department's Information Management Annual Plan (IMAP) include a project for each BCP associated in any way with computer Information Technology, or the BCP will be rejected.

SERVICES REQUESTS 6-0030

Requests for services should be written to the Information Technology Services Division Deputy Director. Information Technology staff will then work with the requestor to develop a preliminary analysis with time and cost estimates.

The Fiscal Forecasting Section has the responsibility to verify the accuracy and potential for attaining identified benefits attributed to Information Technology services for the Medi-Cal Program. The Budget Section has similar responsibility for all other entities in the Department.

OFFICE AUTOMATION AND DECENTRALIZED INFORMATION PROCESSING 6-0040

It is department policy to promote standardization of the Information Technology equipment and software dispersed to programs. The purpose is to promote sharing, improve availability of support, allow for future expansion, and minimize cost.

INFORMATION SECURITY POLICY 6-1000

The Department of Health Services (DHS), as the custodian of confidential and sensitive information (medical, personnel, confidential, etc.), is required to ensure the integrity, availability, accountability, and auditability of these records. The DHS Information Security Policy outlines DHS requirements established to address information security and extends to all DHS personnel, contractors, vendors, clients, and customers.

The DHS Information Security Officer (ISO) will schedule annual security awareness training for all staff. The schedule for training will be available in February 2004 and will be updated annually thereafter.

Please familiarize yourself with the contents of the DHS policy below and sign the acknowledgement. The acknowledgement must be renewed annually and submitted to and retained by your supervisor.

Please e-mail any questions or concerns to Rachael Strider, DHS ISO, at secadmin@dhs.ca.gov or call the DHS Help Desk at (800) 579-0874.

INTRODUCTION 6-1010

The Department of Health Services' (DHS) Information Security Policy provides a general framework that employees shall follow when accessing the State's automated information systems and related devices. Employees should have no reasonable expectation of privacy in the use of these resources. Included with this policy are security requirements from the Information Technology Section of the State Administrative Manual (SAM), Government Code, Department of Information Technology, the DHS Incompatible Activities Statement, labor agreements, and applicable Public Employment Relations Board (PERB) decisions.

DHS INFORMATION SECURITY 6-1010.1

Government Code Section 11771 states: "The chief executive officer of each state agency that uses, receives, or provides information technology services shall designate an Information Security Officer (ISO) who shall be responsible for implementing state policies and standards regarding the confidentiality and security of information pertaining to his or her respective agency. The policies and standards shall include, but are not limited to, strict controls to prevent unauthorized access to data maintained in computer files, program documentation, data processing systems, data files, and data processing equipment physically located in the agency."

The DHS ISO's responsibilities include the following:

• Oversight responsibility for ensuring the integrity and security of automated files and databases (SAM Section 4841.2);

• Oversight of agency compliance with policies and procedures regarding the security of information assets (SAM Section 4841.1);

• Review and approval of all Information Security Incident Reports and oversight of corrective action to remedy the security problem (SAM Section 4845); and

• Oversight of the development of the DHS Operational Recovery Plan (SAM Section 4843).

CLASSIFICATION OF DATA (SAM SECTION 4840.4) 6-1010.2

Automated files and databases should be given appropriate protection from loss, inappropriate disclosure, and unauthorized modification. Files and databases can contain the following types of information:

1. **Public.** Any information prepared, owned, used, or retained by a state agency and not specifically exempt from the disclosure requirements of the California Public Records Act (Government Code, Sections 6250-6255) or other applicable state or federal laws. Public data is suitable for public dissemination and can be easily reproduced from other sources. Protection mechanisms are typically focused on integrity and availability.

2. **Confidential.** Information maintained by state agencies that is exempt from disclosure under the provisions of the California Public Records Act (Government Code, Sections 6250-6265) or other applicable state or federal laws. Under the Information Practices Act (Civil Code, Sections 1798-1798.70), personal information may not be disclosed in a manner that identifies that individual unless authorized by law. Confidential data needs to be protected from unauthorized access or disclosure.

a. **Confidential-Critical.** Privileged data that has the most limited access and requires the highest degree of integrity. This is data that will do the most damage to the organization should it be disclosed.

b. **Confidential-Private.** Data essential to the ongoing operation of the organization and its subsidiaries. It allows the organization to conduct its internal business and maintain support of its applications and business processes. Protection mechanisms are typically focused on the sensitivity of disclosure outside of a business function. Additionally, the availability of the data must support the criticalness of the business function.

c. **Confidential-Restricted.** Data that is intended for internal use within an organization. This data must be protected from unauthorized access, modification, or deletion. Restricted data should only be provided to individuals with a need to know and they must be authorized to access the information. Protection mechanisms are typically focused on the sensitivity of disclosure outside of the organization.

3. **Sensitive Information.** May be either public or confidential and requires special precautions to protect it from unauthorized modifications or deletions.

POLICY MAINTENANCE 6-1010.3

The DHS ISO is responsible for maintaining this policy for DHS. However, final review and approval of policy content is the responsibility of the DHS Director or the Director's designee.

Any comments, questions, corrections, proposals for clarification, or changes to this policy are to be submitted to the DHS ISO.

REGULATION AND ENFORCEMENT 6-1010.4

The DHS Director or the Director's designee is/are responsible for ensuring compliance with provisions of this policy and the administration of the following duties, which include, but are not limited to:

1. Investigating alleged or suspected non-compliance within the provisions of this policy;

2. Suspending service or access to employees when deemed necessary for the operation and/or integrity of the State communications infrastructure or connected networks;

3. Proceeding in accordance with DHS and civil service rules when evidence of non-compliance of this policy is discovered; and

4. Monitoring and/or logging all network activity.

INFORMATION SECURITY STRATEGY 6-1020

An Information Security Strategy is the methodology used to protect the confidentiality, integrity, and security of information assets. This section contains the DHS detailed strategy employees are to follow when using, accessing, or maintaining DHS resources.

GOOD INFORMATION SECURITY PRACTICES 6-1020.1

Good security practices are expected of each employee, which include, but are not limited to:

1. Employees accessing DHS information assets should use due care to preserve data integrity and confidentiality.

2. Employees accessing DHS data should take appropriate precautions to ensure the protection of that data from unauthorized access or destruction.

3. Employees are to use DHS information assets and computer resources for DHS business purposes.

SOFTWARE 6-1020.2

1. All computer software purchased and/or developed by or for DHS is the property of DHS and is to be used for legitimate business purposes only.

2. Computer software should be acquired from reputable sources that will assure the integrity of the software.

3. Software license agreements, terms and conditions, and copyright laws shall be strictly followed.

4. Using shareware and freeware (public domain materials) obtained from online bulletins or other sources must have prior approval from the Division Chief and the DHS ISO.

COMPUTER VIRUSES 6-1020.3

Preventive measures must be taken to prevent malicious software (e.g., computer viruses, worms, Trojan horses, or bacteria) from causing damage to files and operating systems. Therefore, all servers and workstations connected to the DHS network, and/or which store or transmit DHS information must participate in the ITSD centrally managed Symantec Anti-Virus Program.

Employees are not authorized to turn off or disable virus-checking systems. Employees must scan all diskettes or other media for viruses prior to use.

In the case of a possible virus, call the ITSD HelpDesk at (916) 440-7000 or e-mail itsdhelp@dhs.ca.gov to receive proper guidance in analyzing your situation.

INFORMATION SECURITY VIOLATIONS 6-1020.4

Listed below are security violations to be reported to one's supervisor. The supervisor should then complete the Security Incident Report and submit it to the DHS ISO:

- Apparent unauthorized access or attempted unauthorized access to data and systems;
- Apparent theft of information technology equipment;
- Apparent detection of a computer virus on a state computer;
- Apparent malicious damage of equipment, systems, or data; and
- Apparent inappropriate use of DHS computer resources.

Note: A copy of the Information Security Incident Report is available on Attachment A of this policy, the DHS Intranet, or SAM Section 4845.

COMPUTER SECURITY 6-1020.5

Employees are responsible for the security of their computer and their data. The following steps are to be taken to protect computer equipment from theft, unauthorized use, and to ensure that DHS systems and information security are not inadvertently compromised:

1. Contracted personnel or non-DHS employees should not be granted access to the DHS network or any State computer systems, without obtaining prior approval from their Division Chief and notifying the DHS ISO.

2. Employees must not establish local area networks or modem connections, including Point to Point or Serial Line IP connections, on existing local or wide area networks without prior approval from the DHS ISO.

3. Employees must not possess, or attempt to obtain, a network protocol analyzer or similar device (including software) for capturing and/or reading electronic signals from the State's computer network, without prior approval from the DHS ISO.

4. Employees must not possess, or attempt to obtain, password-breaking software (e.g., crack) used to guess employee passwords without prior approval from the DHS ISO.

5. Employees must not intentionally destroy, modify, or release computer programs or data, or introduce malicious code (such as a computer virus).

6. Desktop systems should be kept in secure areas (i.e., a secure building or room) or should be physically attached to a desk or table.

7. The use of surge protectors and lock-down devices is encouraged.

8. When using portable systems (laptops) reasonable measures must be taken to prevent theft (see Attachment B for the Laptop Safety Guidelines.)

9. Removable media should be placed in a secure area when not in use.

10. An appropriate level of back-up is recommended once a week, at a minimum.

11. Confidential or critical data should not be stored on a personal computer (PC) unless adequate security precautions have been taken. If unauthorized access is a concern, the use of security software to password protect the data is encouraged.

12. Unattended PCs are to be protected with something like a password protected screen saver.

BACKUP/RECOVERY PROCEDURES AND OFF-SITE STORAGE 6-1020.6

Having a backup will allow data to be restored in a minimum amount of time. The following steps should be taken to ensure successful data recovery:

1. Files should be copied (backed up) and kept in a secure area;

2. For mission critical systems (SAM Section 4842.11), the backups should be stored at the secured off-site location identified in the Operational Recovery Plan;

3. There should be a regular schedule for making backup copies. The frequency between backups depends on how data files are used and the amount of time that would be required to restore the data should it be lost; and

4. Do not risk more data than can be easily restored. It is recommended that data be backed up at least once a week.

RISK MANAGEMENT PROGRAM – OPERATIONAL RECOVERY PLAN AND RISK ANALYSIS 6-1020.7

1. Operational Recovery Plan (ORP)

A Risk Management Program includes an ORP that addresses what to do if and when a computer and/or the data files are violated, lost, damaged, or inaccessible. An ORP is required for every mission critical application as stated in SAM Section 4843. The ORP contains detailed procedures that will help assure continued agency operations in the event of a disaster.

Responsibility for preparing and updating the ORP resides with each program. The ORP is a tool for the program to recover lost, damaged, or inaccessible information assets.

The ISO is responsible for assembling each program's ORP with "mission critical applications" into a Departmental ORP that is submitted annually to the Department of Information Technology (DOIT).

2. Risk Analysis

A risk analysis should be conducted for each statewide information system, especially those that contain confidential, sensitive, or critical information. The data security review (or risk analysis) will look first at the risks or exposures of an application, and then determine the appropriate set of safeguards/controls for that system. Included in the analysis is a cost or impact of potential losses, along with alternative means of removing or limiting risks. SAM Section 4842.1 describes the risk analysis process.

PASSWORD PROTECTION (SECURING DATA FROM UNAUTHORIZEDACCESS) 6-1020.8

Employees are responsible for the confidentiality and security of their passwords. The following password protection requirements must be met to secure data from unauthorized access:

• Passwords are not to be shared.

• Select an unusual combination of 8 characters or more for a secure password. Avoid words with personal associations, such as names of family members or pets, favorite hobbies, sports, or vacation spots. Non-dictionary words are even more secure.

• Keep passwords confidential, including passwords used for dial-up access. They are not to be written down, posted where they may be accessed, or included in a data file, log-on script, or macro.

• Passwords are to be changed immediately if revealed or compromised.

• Passwords are to be changed every 60 days.

• Any suspected unauthorized use of an ID or password is to be reported to one’s supervisor and the DHS ISO upon discovery.

• When logged on, employees should never leave their computer terminal or workstation unattended unless something like a screen-saver requiring passwords for access is used.

MOBILE COMPUTING POLICY 6-1020.9

PURPOSE/SCOPE

Mobile computing has become an inherent part of doing business at CDHS. Most mobile devices have the capacity to store CDHS owned data. Because data can be portable, CDHS must ensure due diligence is taken to ensure data is protected appropriately.

For the purposes of this Policy, mobile devices are defined as any portable device such as laptops, PDAs, Blackberries, tablet PCs, etc. The term “employee” refers to CDHS employees and non-CDHS employees, including contract employees.

The employee’s Branch Chief and ISO must approve all non-CDHS mobile devices and must meet all of the requirements set forth in this document

All mobile devices used for CDHS business purposes are subject to inspection and possible forensic analysis by the ISO at any time.

ACCEPTABLE USE

An employee agrees to take reasonable precautions for both the security of their mobile device and the information it contains.

1. Upon allocation of a mobile device, the employee agrees to comply with all applicable sections of the CDHS Information Security Policy;

2. All mobile devices issued to employees remain the property of CDHS;

3. Upon termination of employment the individual must return the mobile device to their LAN Administrator or supervisor.

Software

1. All mobile devices must have the CDHS standard anti-virus software installed and security patches up to date. Anti-virus signatures are to be kept up-to-date if the mobile device is to be used off-line (from the CDHS network) for an extended period. See Maintenance section below;

2. Employees must take reasonable steps to protect against the installation of unlicensed or malicious software;

3. Commercial software must be on the ISO and LAN Administrators approved software list;

4. Commercial software must have a valid license for each prospective employee;

5. Commercial software (e.g., shareware, freeware, non-standard software) must be approved by the employee’s Branch Chief and the ISO prior to being installed onto the device;

6. When applicable re-appropriated mobile devices shall be configured with the approved CDHS ITSD build.

Confidential Information

1. Confidential information containing names, social security numbers, medical or financial information should not be downloaded or stored on mobile devices unless absolutely necessary for program operations.

2. In cases where use of mobile devices for downloading or storage of confidential information has been determined to be absolutely necessary, the following criteria must be met:

a. The minimum amount of confidential information should be downloaded or stored,

b. The information must be encrypted,

c. Social security numbers should not be associated with names on mobile devices, if at all possible.

3. In cases where use of mobile devices for downloading or storage of confidential information has been determined to be absolutely necessary, employees must ensure that they use the following deletion and destruction methodology:

a. Employees are required to delete information from their mobile device if it is clearly no longer needed or potentially useful. Use of an "erase" feature (e.g., putting a document in a virtual recycle bin) is not sufficient for confidential information because the information may still be recoverable. Confidential data must be deleted via an overwrite (zeroization) program or other such device approved by the ISO,

b. Prior to disposal, defective or damaged diskettes (e.g., CD-ROM, floppy, tape) containing confidential information must be destroyed using ISO approved methods,

c. Other storage media containing confidential information must be disposed of in the locked destruction bins found in CDHS offices.

Physical Security

1. Mobile devices must not be left unattended at any time. When taken off the worksite premises, mobile devices must not be separated from employee at airports, automobiles, or hotel rooms;

2. When working with mobile devices on the worksite premises, mobile devices are to be cable-locked to an immovable surface or be removed from a docking station and placed in lockable storage whenever the user leaves it.

3. Users must take precautions to ensure other persons cannot view on-screen data in public locations;

4. The identification number of the mobile device should be recorded and kept separately in a safe place. It must not be stored with the mobile device or in the carrying case.

Access Control/Authentication

1. Mobile devices must be protected by a power-on password;

2. When applicable, employees must select a strong password consistent with DHS policy;

3. All non-CDHS mobile devices (i.e., devices belonging to contractors) connecting to the network should meet the following criteria:

a. Must be approved by the ISO and the employees Branch Chief,

b. Connections are only permitted via approved communication paths,

c. At a minimum, all access must be authenticated locally.

4. Employees must use an approved encryption product when storing information with a classification of “Confidential” or higher as classified in SAM;

5. When applicable, a disk drive lock is to be installed with the mobile device;

6. Employees with mobile devices containing confidential data must ensure that they use the following deletion and destruction methodology:

a. Employees are required to delete information from their mobile device if it is clearly no longer needed or potentially useful. Use of an "erase" feature (e.g., putting a document in a virtual recycle bin) is not sufficient for confidential information because the information may still be recoverable. Confidential data must be deleted via an overwrite (zeroization) program or other such device approved by the ISO,

b. Prior to disposal, defective or damaged diskettes (e.g., CD-ROM, floppy, tape) containing confidential information must be destroyed using scissors or other methods approved by the ISO,

c. Other storage media containing confidential information must be disposed of in the locked destruction bins found in CDHS offices.

7. When applicable, mobile devices shall employ an ISO approved software firewall.

Tracking/Recovery

Employees must advise the following parties immediately if their mobile device is lost or stolen:

a. ITSD Helpdesk (who in turn will notify the ISO)

b. Employee’s Manager/supervisor

c. Privacy Office

Maintenance

1. At a minimum, employees are required to return (or make available) the Laptops and Tablet PCs to their LAN Administrator ***monthly*** for regular maintenance (e.g., update anti-virus, updated application and system patches);

2. Blackberries and PDA's are to be tethered to the PC for synchronization and encryption updates ***weekly*** at a minimum.

INTERNET/ELECTRONIC MAIL 6-1030

DHS employees are granted access to Internet and E-mail resources to provide education, research, marketing, procurement, and service opportunities in the performance of their duties. Employees who access Internet and/or E-mail are to follow these guidelines unless required of an employee's position to conduct official DHS business.

CONFIDENTIAL INFORMATION 6-1030.1

Any confidential information sent through the Internet and/or E-mail could be intercepted, modified, misdirected, or destroyed by unauthorized persons if adequate access controls are not in place.

In performing DHS business, the employee shall take every precaution to ensure the security of the information. Confidential information may be transmitted via Internet and/or E-mail only when:

1. Program management approvals have been obtained; and

2. Encryption, authentication, and/or any other DHS ISO approved security schemes and/or policies are used to ensure that data is secured and made available to appropriate and intended recipients only. (SAM Sections 4840-4845 and Health Administrative Manual, Section 3-6040, and Sections 11-3000.)

EMPLOYEE RESPONSIBILITIES 6-1030.2

1. Conduct all Internet and/or E-mail activities in a professional, lawful, and ethical manner, including the use of and development of content for the Internet;

2. Support the use of existing infrastructure, technologies, procedures and standards in using, developing, or making information available on the Internet;

3. Employees may be restricted from participating in mailing lists discussion groups, newsgroups, list servers, or other interactive communications if such participation is excessive or inhibiting overall network performance; and

4. Accessing a personal or private Internet Service Provider for personal use while using any State equipment, or while using non-state equipment for conducting State business, does not in any manner release any entity from the responsibility of complying with this policy.

USE OF INTERNET/E-MAIL RESOURCES 6-1030.3

The intentional use of State time and resources for personal advantage, gain, or profit is inconsistent, incompatible, and in conflict with the duties of officers, contractors, and employees. Examples of inappropriate use include, but are not limited to, viewing, sending, creating, and/or downloading any information that:

1. Violates or infringes on the rights of any other person, including the right to privacy;

2. Contains defamatory, false, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or otherwise biased, discriminatory, or illegal material;

3. Violates agency or departmental regulations prohibiting sexual harassment, and/or discrimination;

4. Restricts or inhibits other users from using the system or the efficiency of the computer systems;

5. Encourages the use of controlled substances; or

6. Utilizes the system for any other illegal purpose. It is also unacceptable for an employee to use the facilities and capabilities of DHS resources to:

1. Conduct, engage, or solicit the performance of any activities in violation of any state, federal or local laws, regulations, rules, executive orders or agency or departmental regulations, policies or directives;

2. Transmit material, information, or software in violation of any local, state or federal law;

3. Conduct any political activity;

4. Conduct any unapproved fundraising or public relations activities;

5. Operate a personal Web Server or make available any Internet services using such server;

6. Engage in any activity for personal gain or personal business transactions;

7. Make any unauthorized purchases; or

8. Use departmental records for private gain, or divulge confidential departmental information or records unless officially authorized to do so.

DIVISION/ PROGRAM RESPONSIBILITIES 6-1030.4

1. Ensure that sufficient resources and appropriate staff are available to establish and maintain Internet activities in a responsible manner;

2. Ensure that web site content is relevant and current including references to non-DHS resources, such as other state or federal agencies;

3. Ensure that all content placed on the Internet, regardless of source of information, is approved in accordance with existing public information release policies and procedures prior to placement on the Internet and/or E-mail;

4. Route Internet or E-mail related Interagency Service Requests through the Information Technology Services Division (ITSD) for approval;

5. Ensure that DHS ISO approved security models are used in implementing security;

6. Define and document security requirements and project specifications prior to initiating Internet or E-mail projects and submit them to ITSD for approval;

7. Ensure that no contracts with, or procurement of, commercial or private Internet Service Providers for either Internet or E-mail activities are made without prior approval from the Chief Information Officer and the DHS ISO; and

8. Ensure that none of the following are established or maintained without obtaining prior approval from the Chief Information Officer and the DHS ISO: Internet/web servers, proxy servers, firewalls, or client browsers configured to access a proxy server.

9. Each Division must designate a representative to participate in the DHS Patch and Vulnerability Group.

TERMINATION (VOLUNTARY OR INVOLUNTARY) 6-1030.5

In the event that an employee is terminating his or her relationship with CDHS, the employee's immediate supervisor is responsible for:

1. Filling out and submitting the employee's exit clearance form.

2. Ensuring all physical property in the custody of the employee including, but not limited to keys, identification cards, software, data and documentation, is returned before the employee leaves CDHS.

3. Notifying LAN Administration that the privileges associated with the employee's user ID must be revoked.

4. Terminating all other work-related privileges of the employee at the time that the termination takes place.

SYSTEM SECURITY OPERATION 6-1040

PATCH AND VULNERABILITY MANAGEMENT 6-1040.1

LAN/System Administrators must apply all vendor recommended bug fixes, service packs and security patches (e.g. Microsoft, Cisco) on operating systems, applications, and/or hardware appliances as prescribed by the patch application process defined by the Patch and Vulnerability Group. (PVG)

• The DHS ISO will monitor relevant security issues, both internally and externally, and will manage the release of security patches on behalf of DHS.

• The PVG will work with appropriate LAN/System Administrators to test security patches before release, where practical.

• Security patches must be implemented within the timeframe specified by the PVG.

CENTRALIZED SYSTEM MANAGEMENT SERVER PROGRAM 6-1040.2

To ensure that critical security updates are quickly and effectively applied and to improve operational efficiency, all servers and workstations connected to the DHS network, and/or which store or transmit DHS information must participate in the ITSD centrally managed System Management Server (SMS) Program.

REMOTE ACCESS 6-1040.3

To ensure that the requirements for remote access are consistently observed, the ISO reserves the right to conduct audits of employees with remote access privileges. These audits could include visits to remote sites (but not an employee's personal residence) as well as a review of the contents of a computer used to access CDHS systems.

Security requirements must be followed at remote locations, although they may be implemented in different ways. For example, paper-based Confidential and Sensitive information needs to be locked up when not in active use. When traveling, a locking briefcase might be employed.

1. **Inbound Connections to CDHS Networks:** All inbound connections and connection methods to CDHS internal networks and/or multi-user computer systems must be ISO approved remote access solutions.

2. **Authentication:** Remote access to CDHS computers and networks requires that all employees be authenticated by identification systems approved by the ISO. All employees working remotely must connect to CDHS computers and internal networks via authorized communications.

3. **Discarding Confidential Information When Off Site:** Employees must not discard confidential information in home or hotel wastebaskets or publicly accessible trash containers. Instead, this information must be retained until it can be shredded, or destroyed using other approved methods.

SERVER HARDENING 6-1040.4

All servers must adhere to ISO approved Server Configuration and Hardening Standards.

SERVER CONFIGURATIONS AND HARDENING 6-1040.5

All servers must adhere to ISO approved Server Configuration and Hardening Standards.

SYSTEM UPGRADES 6-1040.6

Only Authorized employees are permitted to perform system upgrades (e.g., LAN Administrators, approved IT personnel).

All system upgrades (i.e., servers, routers, firewalls, etc.) must adhere to the Change Control Policy.

All computer and communication systems used for production processing at DHS must employ a formal change control process to ensure that only authorized changes are made. This process must include a mechanism for documenting and approving all changes to production computing systems including all significant changes to software, hardware, communications networks, and related procedures.

CHANGE CONTROL DOCUMENTATION 6-1040.8

1. **Hardware, Communications Networks, Operating Systems and Systems Software:** Prior to being installed, new or different versions of hardware, communications networks, operating systems and related systems software for networked production computers must go through the established change control process.

2. **Application (Executable) Programs:** Executable programs provided by external entities must be tested before installation on any DHS production system. Such testing and examination must be consistent with DHS standards and must also be properly documented.

3. **Security Fixes:** All security problem fix software, command scripts, and the like provided by operating system vendors, official computer security incident response programs (CSIRPs), and other third-parties must be tested prior to installation.

NETWORK SECURITY OPERATIONS 6-1050

USER ACCOUNTABILITY 6-1050.1

Accountability must be maintained for all access to system resources through audit trails of employee activity. See ISO Audit Trails Standard.

ACCESS CONTROL 6-1050.2

All workstations and network communication systems used for DHS business activity, no matter where they are located, must utilize an access control system approved by the DHS ISO to ensure that confidential or sensitive information is not improperly disclosed, modified, deleted, or rendered unavailable. Employees must comply with all applicable state and federal privacy requirements when accessing DHS systems.

An approval process that grants access to networked DHS computer and communications systems based on an employee's job responsibilities must be in place.

FIREWALL 6-1050.3

All connections between DHS internal networks and the internet (including other state agencies or any other publicly accessible computer network) must include an approved firewall or related access control system. The privileges that will be permitted via this firewall or related access control system will be based on business needs.

1. All firewalls must be maintained by centralized ITSD.

2. All firewalls used to protect DHS' internal network must run on separate dedicated computers. These computers may not serve any other purposes (such as acting as web servers).

3. Firewall configuration rules and permissible service rules may not be changed without following formal Change Management Procedures and prior approval of the DHS ISO.

4. Firewall configurations must be periodically checked to ensure that they have not changed during software modifications or re-booting of equipment.

GLOSSARY OF TERMS 6-1060

AUTHENTICATION: a systematic way for establishing proof of identity between two or more entities, such as users and hosts. Authentication is often a prerequisite to allowing access to network resources.

ENCRYPTION: the process of converting data from an easily understandable form to what appears to be random, useless gibberish, using mathematical processes that are difficult or impossible to duplicate without knowledge of how the encryption was accomplished.

FIREWALL: a network device or collection of devices that protect inside "trusted" networks from external "untrusted" networks like the Internet, using a variety of technical processes.

INTEGRITY: a characteristic of data relating to its level of corruption or damage; data with questionable integrity may have been corrupted to some degree.

INTERNET AND E-MAIL RESOURCES: include staff, hardware, software, and supporting infrastructure.

MISSION CRITICAL: defined in the State Administrative Manual (SAM), Section 4842.11, as an application that is so important to the State that the loss or unavailability of the application is unacceptable. With a critical application, even short-term unavailability of the information provided by the application would have a significant negative impact on the health and safety of the public or State workers; on the fiscal or legal integrity of state operations; or on the continuation of essential agency programs.

NETWORK ACTIVITY: personal computers, data packets, electronic files, printed materials electronic mail, data records, website communication, password sharing, software, hardware, modem or any other related items or functions performed using State property or conducting State business.

NETWORK PROTOCOL ANALYZER (sniffer): a program often installed on computer networks (usually by a hacker) that gathers information from packets traversing the network and forwards it to the hacker. Sniffers are useful for conducting network reconnaissance, and can help a hacker capture passwords and usernames for use in a later hacking attack. The potential installation of sniffer programs in one of the main reasons that untested software should not be installed by users on their computer systems.

PROXY SERVER: a firewall mechanism that replaces the Internet Protocol (IP) address of a host on the internal (protected) network with its own IP address for all traffic passing through it.

POLITICAL ACTIVITY: affairs pertaining to works or efforts associated with endorsing and/or promoting a political bias not supported by DHS.

REMOVABLE MEDIA: floppy disks, compact discs, or other removable device that contain data.

RIGHT TO PRIVACY: The Privacy Act, passed by Congress in 1974, establishes certain controls over what personal information is collected by the federal government and how it is used. The Act guarantees three primary rights: (1) the right to see records about yourself, subject to the Privacy Act's exemptions, (2) the right to amend that record if it is inaccurate, irrelevant, untimely, or incomplete, and (3) the right to sue the government for violations of the statute including permitting others to see your records (i.e., personnel, medical, and other files involving personal privacy) unless specifically permitted by the Act.

SECURITY AND CONFIDENTIALITY STATEMENT 6-1070

The State Administrative Manual, Section 4842.2 under Personnel Practices requires that all employees receive training on the Department's information security policies, and sign acknowledgments of their security responsibility. The Security and Confidentiality Statement provides the Department with a standardized procedure for documenting this process.

Managers and supervisors should maintain signed statements in their unit files for all employees using or otherwise having access to departmental data systems and information.

SECURITY AND CONFIDENTIALITY ACKNOWLEDGEMENT 6-1070.1

ATTACHMENT A: INFORMATION SECURITY INCIDENT REPORT 6-1080

Employee Computer Security Incident Reporting Form

Use this form to report incidents to the Information Security Office. Programs should send an electronic copy to secadmin@dhs.ca.gov. This form outlines the basic information that the Information Security Office needs to investigate a security incident.